Boost your Hardware RE with glscopeclient

Andrew D. Zonenberg
@azonenberg

hardwear.io USA 2021

IOActive®

Introduction

IOActive®

Structure of this session

- 30 mins of intro / background
- 30 mins of interactive demo

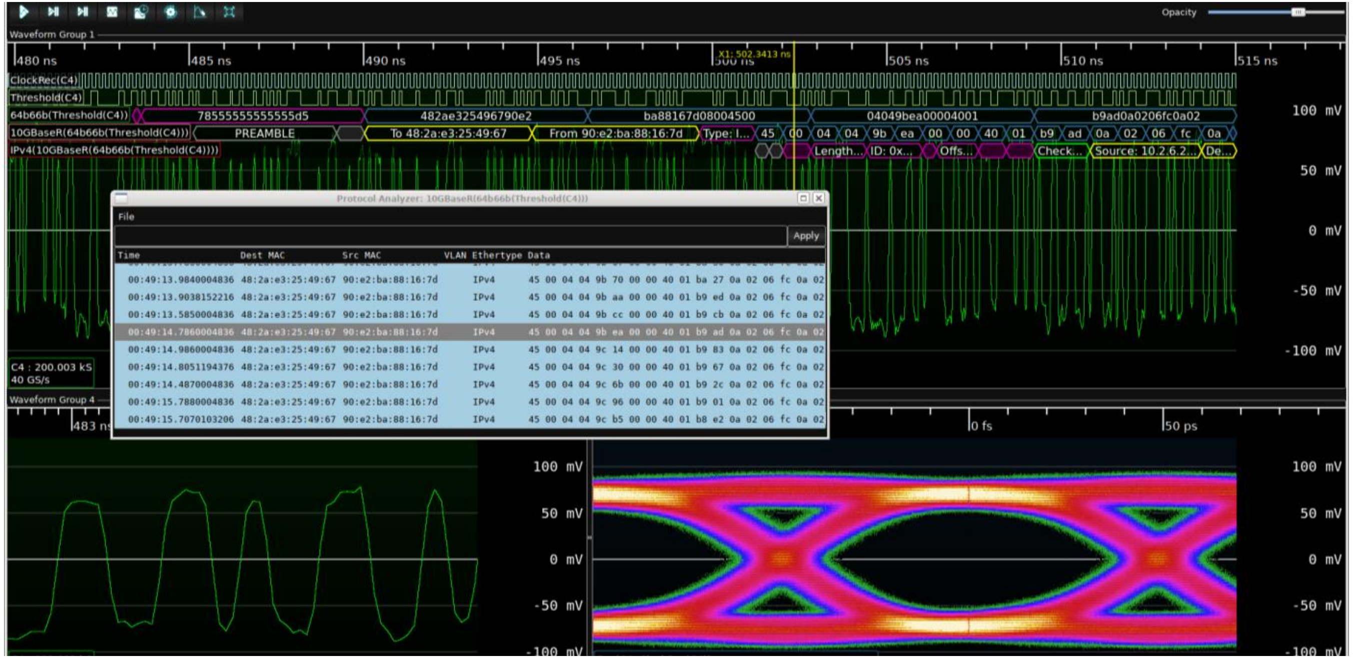
About Me

- Ph.D CS RPI ’15
  - Did my thesis on SoC architecture for security
- IOActive since then
- Lots of GPGPU, HPC, FPGA, optimization, etc
- Started work on what is now glscopeclient around 2011

IOActive and glscopeclient

- Spare time open-source project, not IOA product
  - I’m presenting on company time, so their logo is on my slides
- Recently became stable enough for me to use at work
  - Wrote several decodes to aid embedded pentest projects
  - Hoping to make it useful to the broader community

Sneak peek before we get into details…



```
Time                Dest MAC          Src MAC           VLAN Ethertype Data
  00:49:13.9840004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b 70 00 00 40 01 ba 27 0a 02 06 fc 0a 02
  00:49:13.9038152216 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b aa 00 00 40 01 b9 ed 0a 02 06 fc 0a 02
  00:49:13.5850004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b cc 00 00 40 01 b9 cb 0a 02 06 fc 0a 02
  00:49:14.7860004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b ea 00 00 40 01 b9 ad 0a 02 06 fc 0a 02
  00:49:14.9860004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 14 00 00 40 01 b9 83 0a 02 06 fc 0a 02
  00:49:14.8051194376 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 30 00 00 40 01 b9 67 0a 02 06 fc 0a 02
  00:49:14.4870004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 6b 00 00 40 01 b9 2c 0a 02 06 fc 0a 02
  00:49:15.7880004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 96 00 00 40 01 b9 01 0a 02 06 fc 0a 02
  00:49:15.7070103206 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c b5 00 00 40 01 b8 e2 0a 02 06 fc 0a 02
```

What is glscopeclient?

- GPU accelerated rewrite of unreleased “scopeclient”
  - New frontend with emphasis on performance and scalability
  - Based on same core: libscopehal and libscopeprotocols
- Test equipment remote control
- Waveform analysis
- Permissively licensed (3-clause BSD)
  - Interop w/ commercial tooling is an explicit goal

Release timeline

- **Prerelease:** just build current git master
- **v0.1:** First official release, 1-2 months out?
- **v0.2:** Q4 ‘21 – Q1 ‘22?
  - Lots of cleanup and portability fixes
  - More complete support of various instrument features
  - Finishing incomplete protocol decodes, more validation
  - Maybe OSX support?
- **v1.0:** who knows?

Target platforms

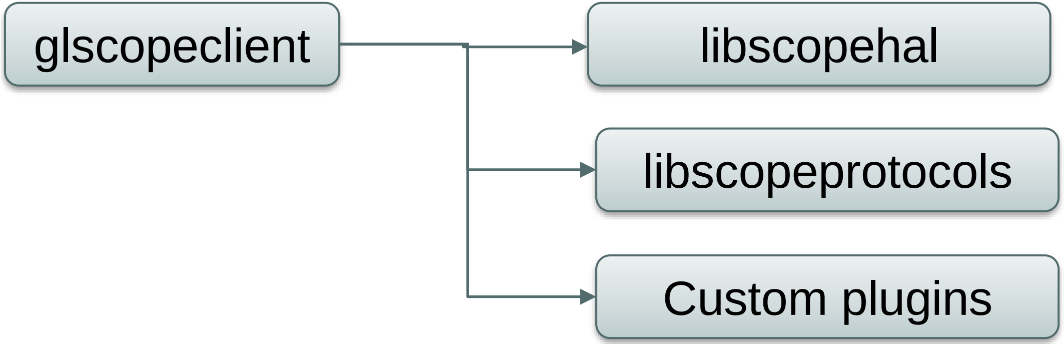
- Linux
  - WIP packaging for Arch, RHEL/CentOS
  - Debian packages created, working on upstreaming
- Windows
  - Already in MinGW repository
  - Alpha release of binary MSI packaging
- 64-bit x86 only (for now)
  - ARM64 planned for mid term, maybe v0.2

Unsupported platforms

- OSX
  - Need to rewrite / port most of renderer to work around graphics stack issues (y u deprecate open standard APIs?)
- Most hypervisors
  - Requires OpenGL 4.3 and compute shaders
    - No emulated GPU provides this AFAIK
  - PCIe passthrough / SR-IOV GPU should work, but untested

Architecture

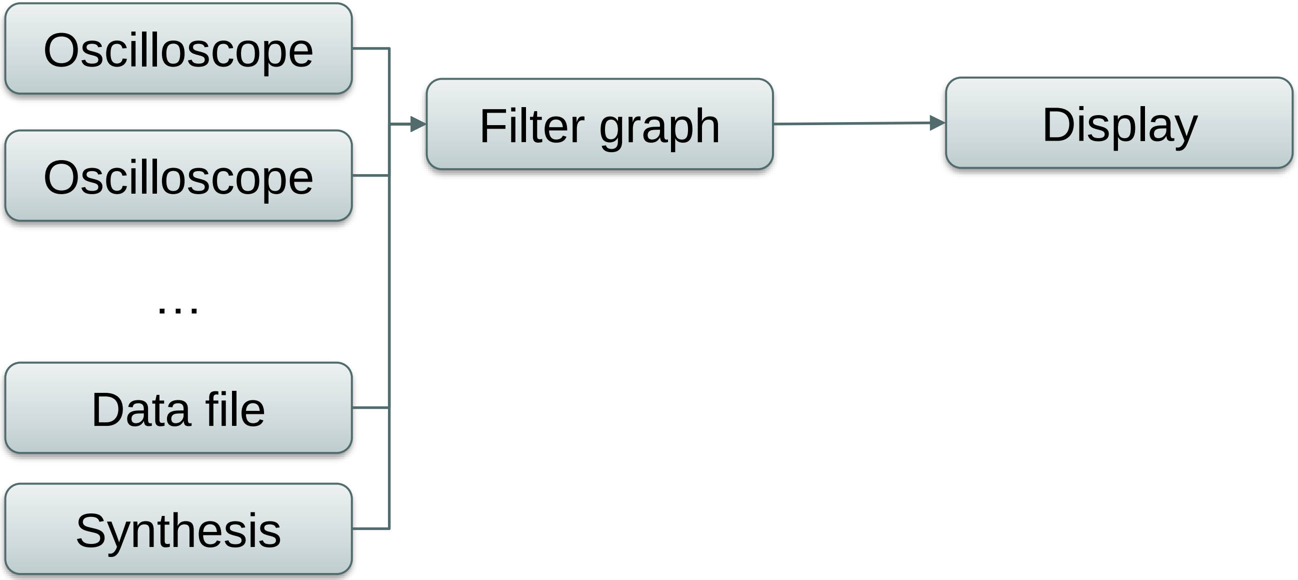
Components



Custom C++ tooling can also call the libraries directly

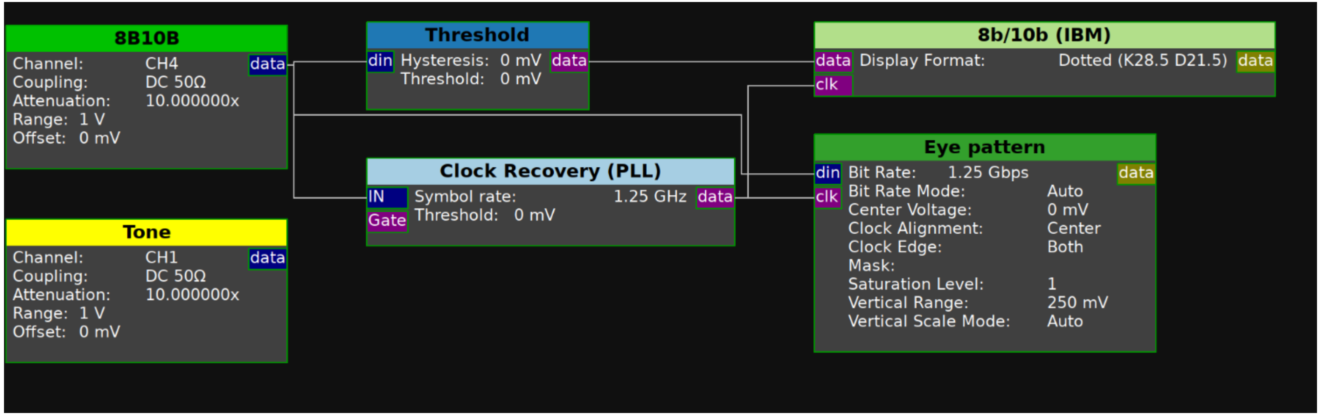
Here be dragons: *no ABI stability for v0.x series!!*

Dataflow


Oscilloscope
Oscilloscope
…
Data file
Synthesis
Filter graph
Display

Filter graphs

- Common DSP/multimedia architecture (like GNU Radio)
- DAG of processing blocks



8B10B
Channel: CH4
Coupling: DC 50Ω
Attenuation: 10.000000x
Range: 1 V
Offset: 0 mV

Tone
Channel: CH1
Coupling: DC 50Ω
Attenuation: 10.000000x
Range: 1 V
Offset: 0 mV

Threshold
Hysteresis: 0 mV
Threshold: 0 mV

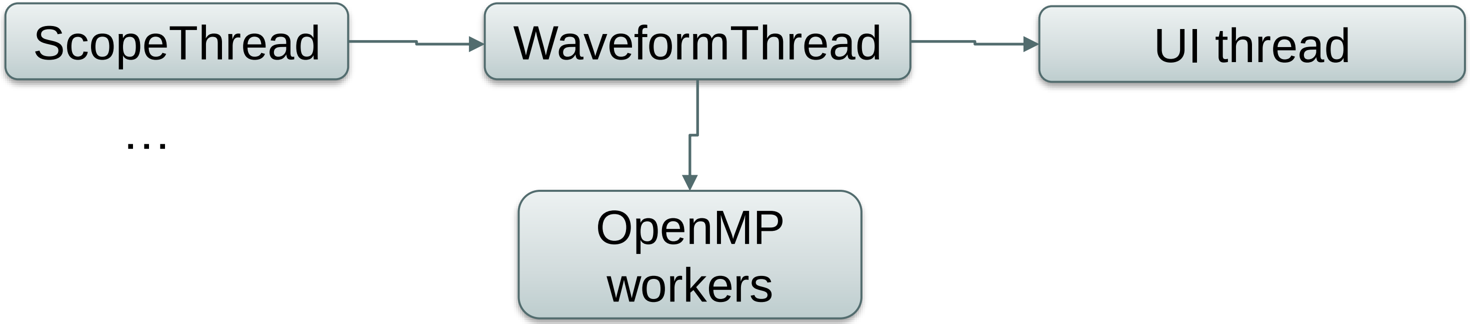
Clock Recovery (PLL)
Symbol rate: 1.25 GHz
Threshold: 0 mV

8b/10b (IBM)
Display Format: Dotted (K28.5 D21.5)

Eye pattern
Bit Rate: 1.25 Gbps
Bit Rate Mode: Auto
Center Voltage: 0 mV
Clock Alignment: Center
Clock Edge: Both
Mask:
Saturation Level: 1
Vertical Range: 250 mV
Vertical Scale Mode: Auto

Threading model

- Filter graph uses custom scheduler + OpenMP
  - Blocks with no dependencies can execute concurrently



File Formats

- Native:
  - .scopesession format
- Import:
  - Agilent / Keysight / Rigol binary
  - CSV (with support for Digilent WaveForms metadata)
  - VCD
  - WAV
- Export:
  - Protocol dumps to CSV

Supported Hardware

DIGILENT®

- They sent me free hardware!
  - … but I haven’t had time to touch it yet ☹
- Coming soon:
  - Analog Discovery 2
  - Analog Discovery Pro 3000
  - Digital Discovery

KEYSIGHT TECHNOLOGIES

Agilent Technologies

- DSO5000
- DSO/MSO6000 (no digital channel support)
- DSO/MSO7000? (untested but probably works)
- MSOX-2000
- MSOX-3000 / 3000T

pico® Technology

- 6000E: usable but missing a few bits
  - No advanced triggers, basic level trigger only
  - No function generator support
- 5000D: early WIP, nothing merged yet
- 3000D: most stuff
- No 2000 or 4000 series support yet, but pending

RIGOL
Beyond Measure

- DS1000Z
- DS1100D/E
- MSO5000

ROHDE & SCHWARZ

- RTM3000 (in progress)

SIGLENT®

- SDS2000X+ (works well, but no MSO support yet)
- SDS5000X (lightly tested)
- SDS6000X? (untested, should work)
- Early SDS1000 driver in the works, not yet merged

TELEDYNE LECROY
Everywhereyoulook™

- All MAUI based scopes use the same command set!
  - Ultra low end (WaveAce etc) are OEM rebrands, not supported
  - *Windows CE WaveSurfers have a few quirks still
- Tested on:
  - DDA5000A
  - HDO9000
  - SDA 8Zi
  - WaveSurfer 3000*
  - WaveRunner Xi / 8000

Tektronix®

- MSO6
- MSO5 (untested but same command set as MSO6)
- MSO4 (untested but same command set as MSO6)

Performance

Factors affecting waveform capture rate

- CPU / FPGA throughput on scope
- Interface bandwidth
  - USB2 / 100baseTX are slow
  - 1000baseT better
  - USB3 / 10GbE / PCIe best
  - Optimize for less round trips and commands
- CPU throughput on host
  - General software optimization techniques here

Scaling issues

- Most entry level scopes: O(1) term dominates
  - Rigol MSO5354: can’t get >1 WFM/s at any mem depth, but respectable throughput of 48 Mbps w/ 50M points
- Higher end scopes: O(n) term dominates
  - Agilent MSO6034A 1ch: 33 WFM/s @ 1K pts, 3.7 @ 1M
  - LeCroy WR8404 2ch: 40 WFM/s @ 80K pts, 3.15 @ 8M

Typical performance with shallow memory

Model	CH	Points	WFM/s	Mbps
Agilent MSO6034A	4	1K	33.0	1
Keysight MSOX3104T	4	2.5K	2.5	<1
PicoScope 6824E	8	100K	33.1	212
Rigol MSO5354	4	10K	1.0	<1
Tektronix MSO64	2	50K	7.0	5
Teledyne LeCroy HDO9204	2	100K	35.0	112
Teledyne LeCroy WR8404M-MS	2	80K	40.0	51

Typical performance with longer memory

Model	CH	Points	WFM/s	Mbps
Agilent MSO6034A	4	1M	1.0	32
Keysight MSOX3104T	4	2M	0.5	32
PicoScope 6824E	4	1M	30.5	1952
Rigol MSO5354	4	1M	0.6	19
Tektronix MSO64	4	500K	3.9	62
Teledyne LeCroy HDO9204	4	1M	5.9	374
Teledyne LeCroy WR8404M-MS	2	800K	16.5	211

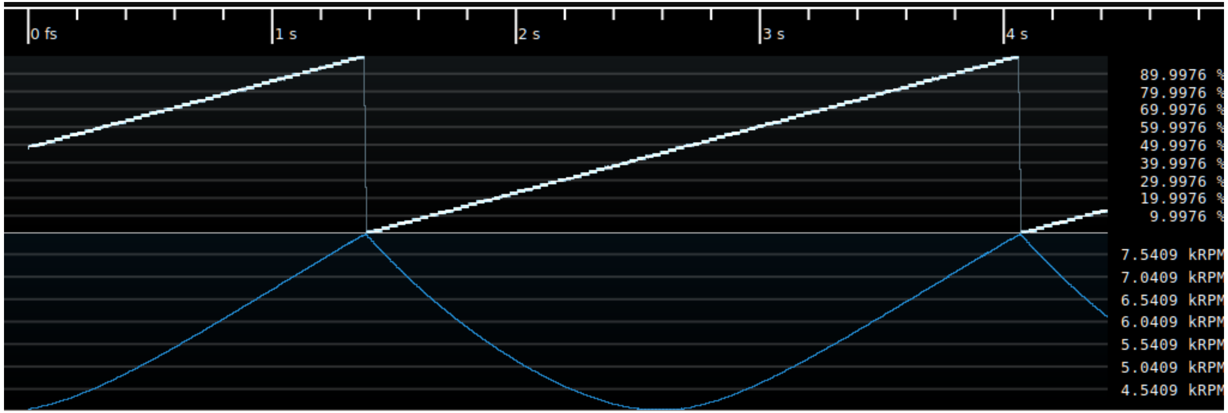
Other performance considerations

- Rendering is GPU performance limited
  - More samples on screen = slower
  - 50 ms to render complete 128M point trace on RTX 2080 Ti
- Filter graph complexity
  - Sequential chains of filters can’t multithread
  - Large FIR filters or FFTs are numerically intensive
  - Availability of OpenCL / AVX2 / AVX512

Capabilities

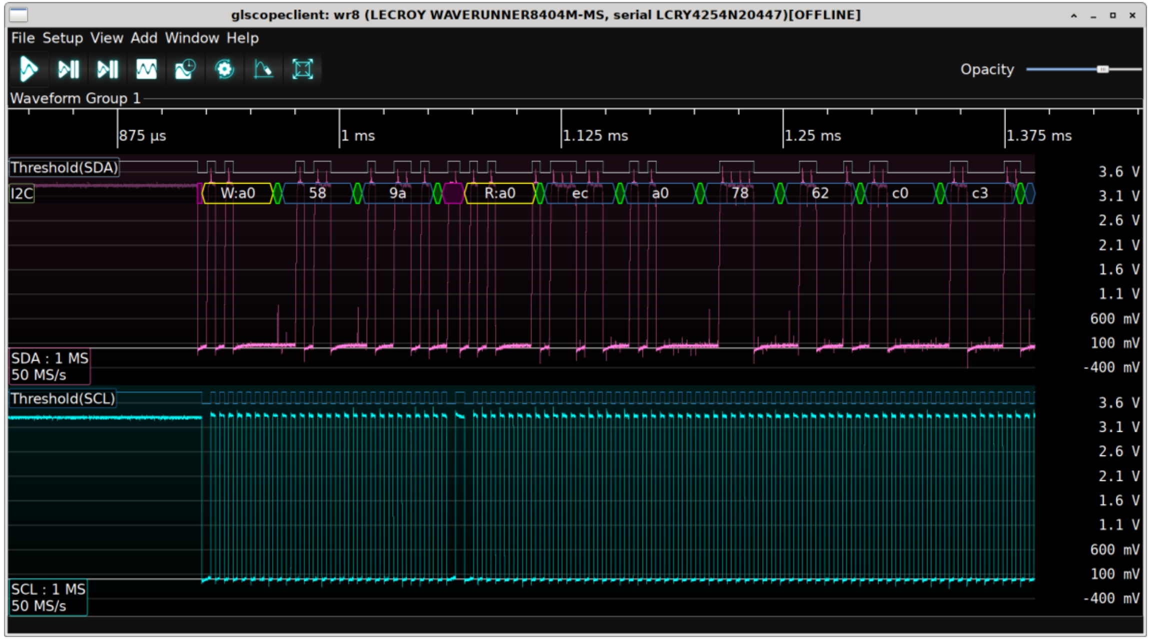
Math / DSP

- AC couple
- Autocorrelation
- DC offset
- Deskew
- Histogram
- Moving average
- Multiply
- Subtract
- Threshold
- Up/down sample



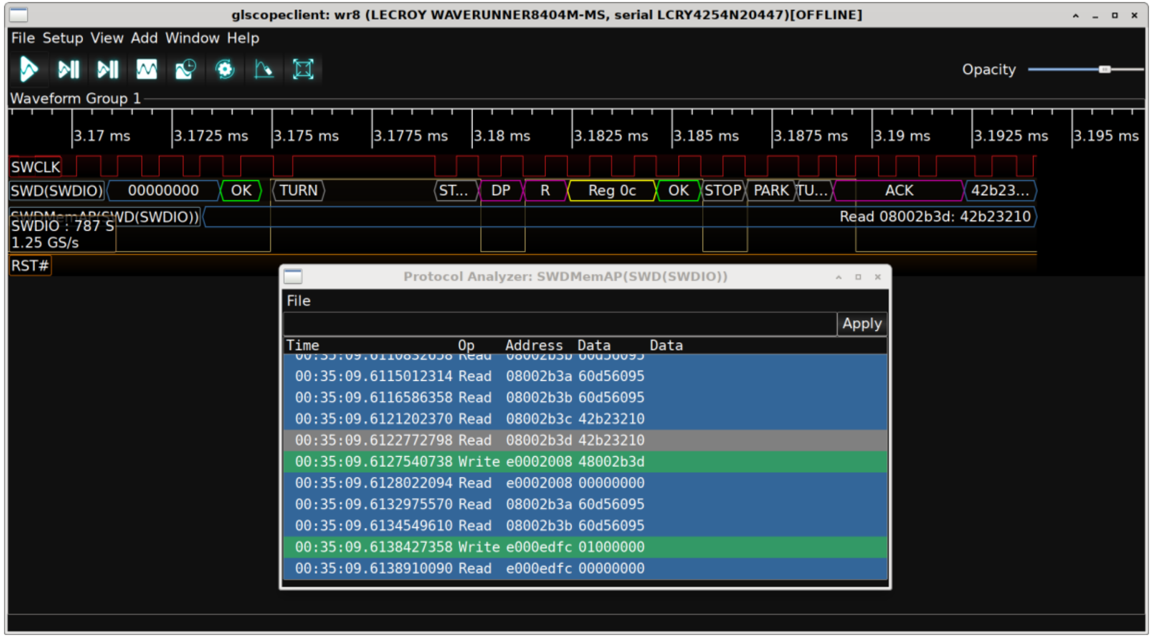
Basic embedded

- 1-wire
- CAN
- I2C
- MIL-STD-1553
- QSPI
- SPI
- UART



Debug

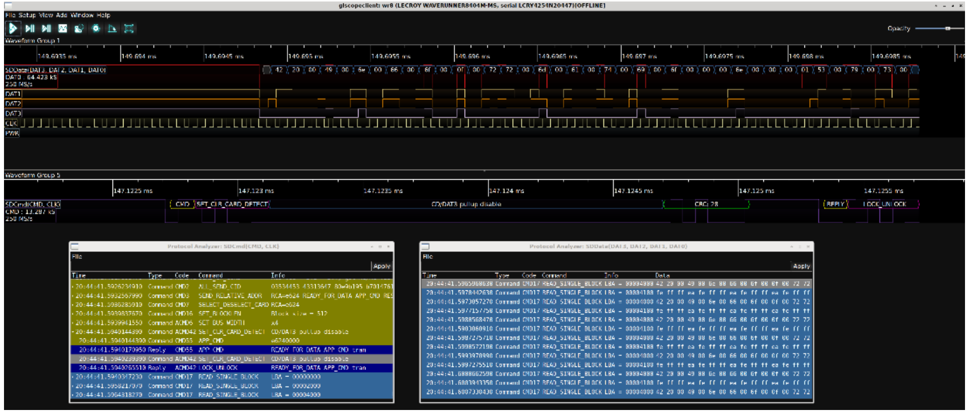
- JTAG
- SWD
- SWD MEM-AP



```
Time                Op    Address  Data     Data
00:35:09.6115012314 Read  08002b3a 60d56095
00:35:09.6116586358 Read  08002b3b 60d56095
00:35:09.6121202370 Read  08002b3c 42b23210
00:35:09.6122772798 Read  08002b3d 42b23210
00:35:09.6127540738 Write e0002008 48002b3d
00:35:09.6128022094 Read  e0002008 00000000
00:35:09.6132975570 Read  08002b3a 60d56095
00:35:09.6134549610 Read  08002b3b 60d56095
00:35:09.6138427358 Write e000edfc 01000000
00:35:09.6138910090 Read  e000edfc 00000000
```

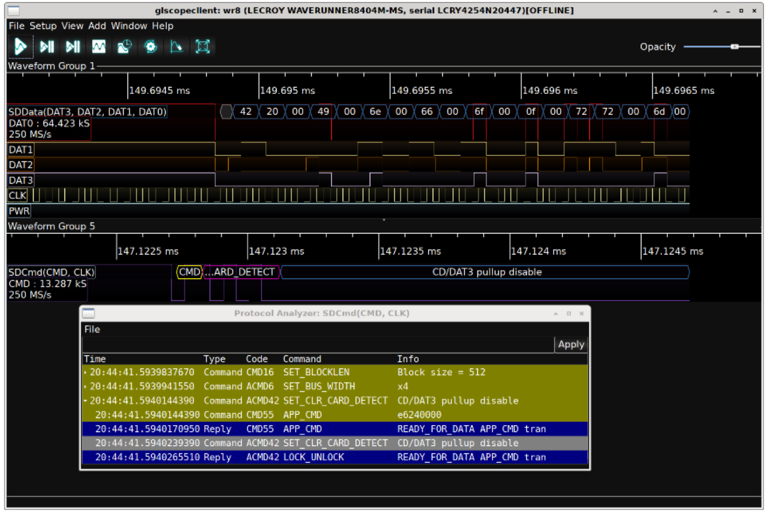
Memory

- DDR1 command bus
- DDR3 command bus
- I2C EEPROM
- SD card cmd / data
- SPI flash



```
Time                 Type    Code   Command              Info
 20:44:41.5926234910 Command CMD2   ALL_SEND_CID         03534453 43313647 80e9b195 b7014761
 20:44:41.5932567990 Command CMD3   SEND_RELATIVE_ADDR   RCA=e624 READY_FOR_DATA APP_CMD RES
 20:44:41.5936285910 Command CMD7   SELECT_DESELECT_CARD RCA=e624
 20:44:41.5939837670 Command CMD16  SET_BLOCKLEN         Block size = 512
 20:44:41.5939941550 Command ACMD6  SET_BUS_WIDTH        x4
 20:44:41.5940144390 Command ACMD42 SET_CLR_CARD_DETECT  CD/DAT3 pullup disable
  20:44:41.5940144390 Command CMD55 APP_CMD              e6240000
  20:44:41.5940170950 Reply   CMD55 APP_CMD              READY_FOR_DATA APP_CMD tran
  20:44:41.5940239390 Command ACMD42 SET_CLR_CARD_DETECT CD/DAT3 pullup disable
  20:44:41.5940265510 Reply   ACMD42 LOCK_UNLOCK         READY_FOR_DATA APP_CMD tran
 20:44:41.5940347230 Command CMD17  READ_SINGLE_BLOCK    LBA = 00000000
 20:44:41.5958217070 Command CMD17  READ_SINGLE_BLOCK    LBA = 00002000
 20:44:41.5964318270 Command CMD17  READ_SINGLE_BLOCK    LBA = 00004000
```

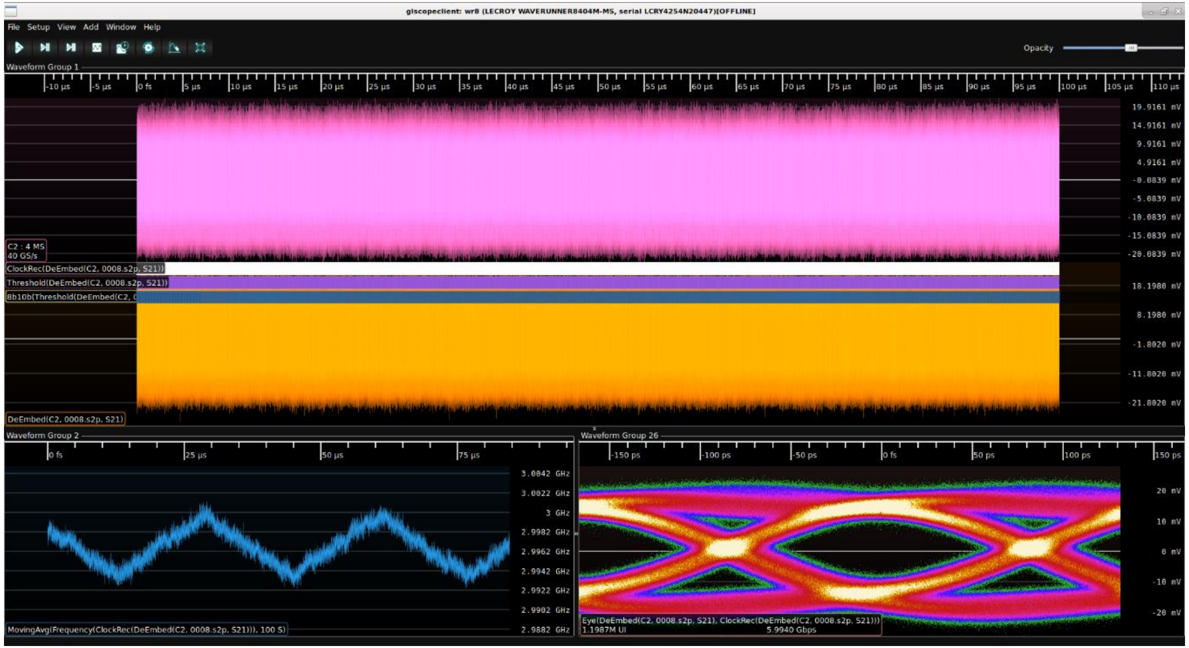
```
Time                Type    Code  Command           Info             Data
20:44:41.5965960630 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.5970442630 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.5973057270 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.5977157750 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.5980568470 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.5983060910 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.5987275710 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.5990572190 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.5993970990 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.5997275510 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.6000662590 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
20:44:41.6003943350 Command CMD17 READ_SINGLE_BLOCK LBA = 00004100 fe ff ff ea fe ff ff ea fe ff ff ea fe ff ff
20:44:41.6007330430 Command CMD17 READ_SINGLE_BLOCK LBA = 00004000 42 20 00 49 00 6e 00 66 00 6f 00 0f 00 72 72
```



```
Time                 Type    Code   Command              Info
 20:44:41.5939837670 Command CMD16  SET_BLOCKLEN         Block size = 512
 20:44:41.5939941550 Command ACMD6  SET_BUS_WIDTH        x4
 20:44:41.5940144390 Command ACMD42 SET_CLR_CARD_DETECT  CD/DAT3 pullup disable
  20:44:41.5940144390 Command CMD55  APP_CMD             e6240000
  20:44:41.5940170950 Reply   CMD55  APP_CMD             READY_FOR_DATA APP_CMD tran
  20:44:41.5940239390 Command ACMD42 SET_CLR_CARD_DETECT CD/DAT3 pullup disable
  20:44:41.5940265510 Reply   ACMD42 LOCK_UNLOCK         READY_FOR_DATA APP_CMD tran
```

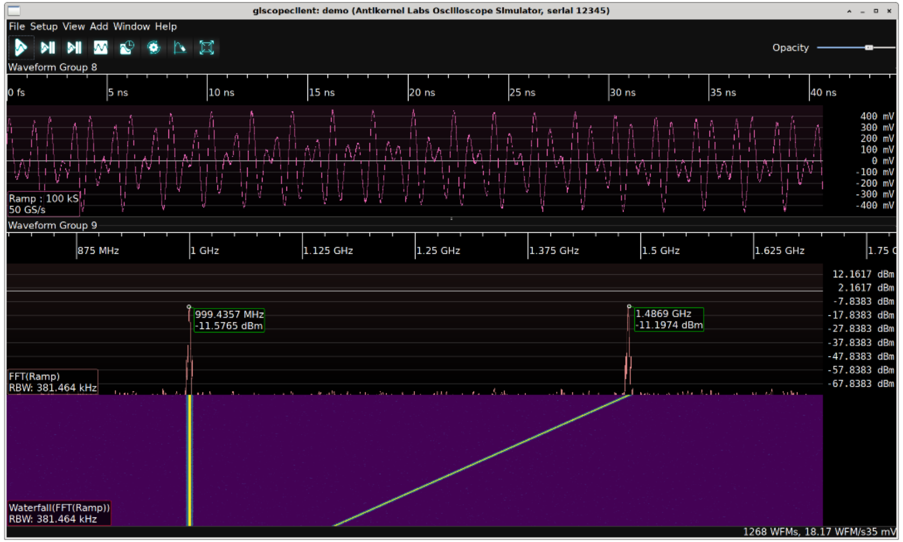
High speed serial

- CDR PLL
- 8B/10B
- 64B/66B



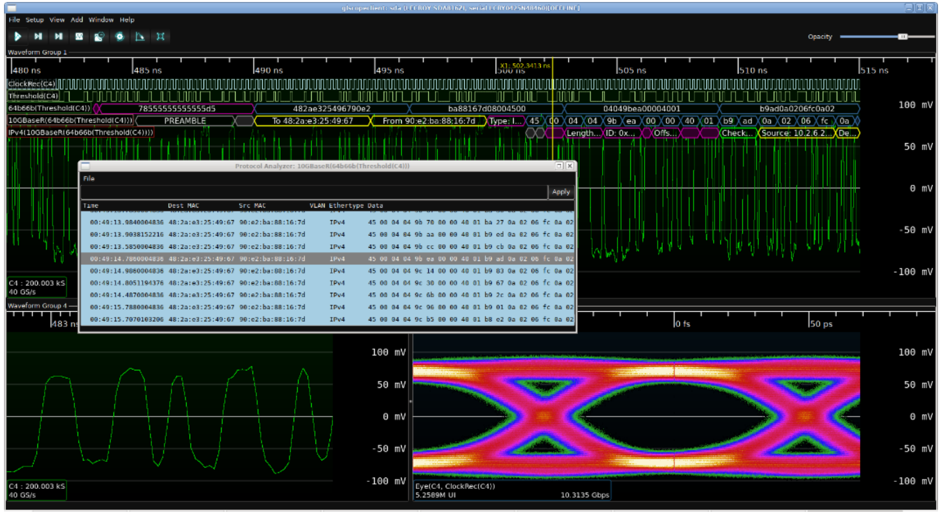
RF / power analysis

- Digital downconversion
- FFT
- FIR filter
  - Low / high pass
  - Band pass / notch
- Phase and frequency vs time
- Spectrogram
- Waterfall

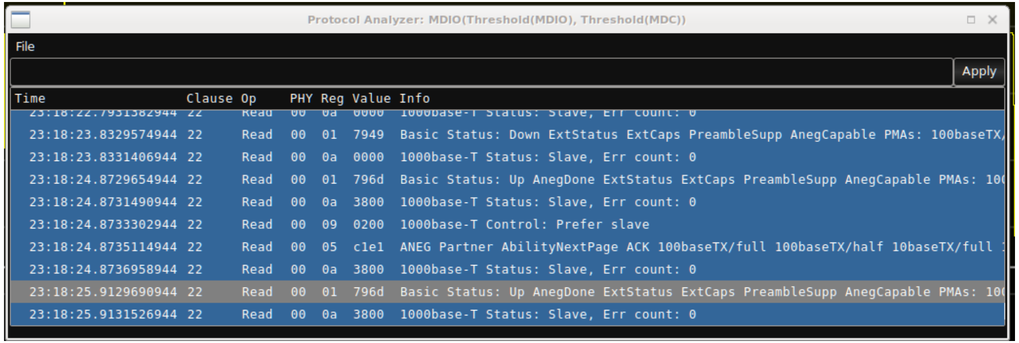


Networking

- 10base-T
- 100base-TX
- 1000base-X
- 10Gbase-R
- Base-T autonegotiation
- GMII
- RGMII
- MDIO



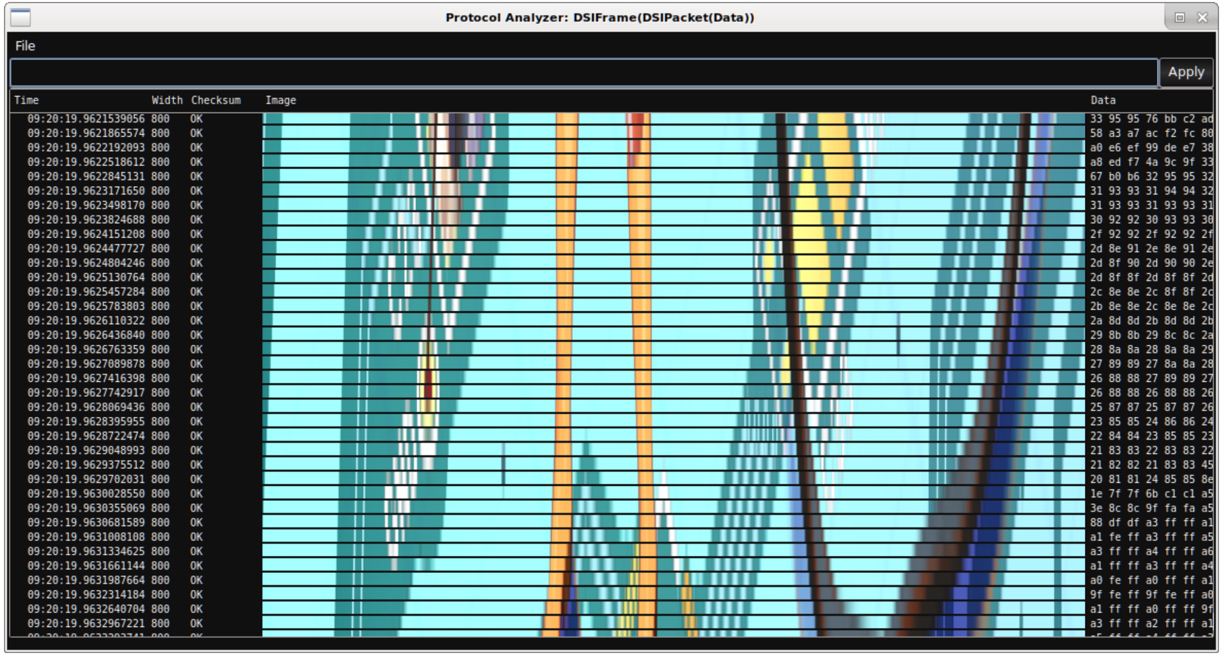
```
Time                Dest MAC          Src MAC           VLAN Ethertype Data
00:49:13.9840004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b 70 00 00 40 01 ba 27 0a 02 06 fc 0a 02
00:49:13.9038152216 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b aa 00 00 40 01 b9 ed 0a 02 06 fc 0a 02
00:49:13.5850004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b cc 00 00 40 01 b9 cb 0a 02 06 fc 0a 02
00:49:14.7860004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9b ea 00 00 40 01 b9 ad 0a 02 06 fc 0a 02
00:49:14.9860004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 14 00 00 40 01 b9 83 0a 02 06 fc 0a 02
00:49:14.8051194376 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 30 00 00 40 01 b9 67 0a 02 06 fc 0a 02
00:49:14.4870004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 6b 00 00 40 01 b9 2c 0a 02 06 fc 0a 02
00:49:15.7880004836 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c 96 00 00 40 01 b9 01 0a 02 06 fc 0a 02
00:49:15.7070103206 48:2a:e3:25:49:67 90:e2:ba:88:16:7d      IPv4      45 00 04 04 9c b5 00 00 40 01 b8 e2 0a 02 06 fc 0a 02
```



```
Time                Clause Op   PHY Reg Value Info
23:18:22.7931382944 22     Read 00  0a  0000  1000base-T Status: Slave, Err count: 0
23:18:23.8329574944 22     Read 00  01  7949  Basic Status: Down ExtStatus ExtCaps PreambleSupp AnegCapable PMAs: 100baseTX/
23:18:23.8331406944 22     Read 00  0a  0000  1000base-T Status: Slave, Err count: 0
23:18:24.8729654944 22     Read 00  01  796d  Basic Status: Up AnegDone ExtStatus ExtCaps PreambleSupp AnegCapable PMAs: 10(
23:18:24.8731490944 22     Read 00  0a  3800  1000base-T Status: Slave, Err count: 0
23:18:24.8733302944 22     Read 00  09  0200  1000base-T Control: Prefer slave
23:18:24.8735114944 22     Read 00  05  c1e1  ANEG Partner AbilityNextPage ACK 100baseTX/full 100baseTX/half 10baseTX/full 1
23:18:24.8736958944 22     Read 00  0a  3800  1000base-T Status: Slave, Err count: 0
23:18:25.9129690944 22     Read 00  01  796d  Basic Status: Up AnegDone ExtStatus ExtCaps PreambleSupp AnegCapable PMAs: 10(
23:18:25.9131526944 22     Read 00  0a  3800  1000base-T Status: Slave, Err count: 0
```

Mobile

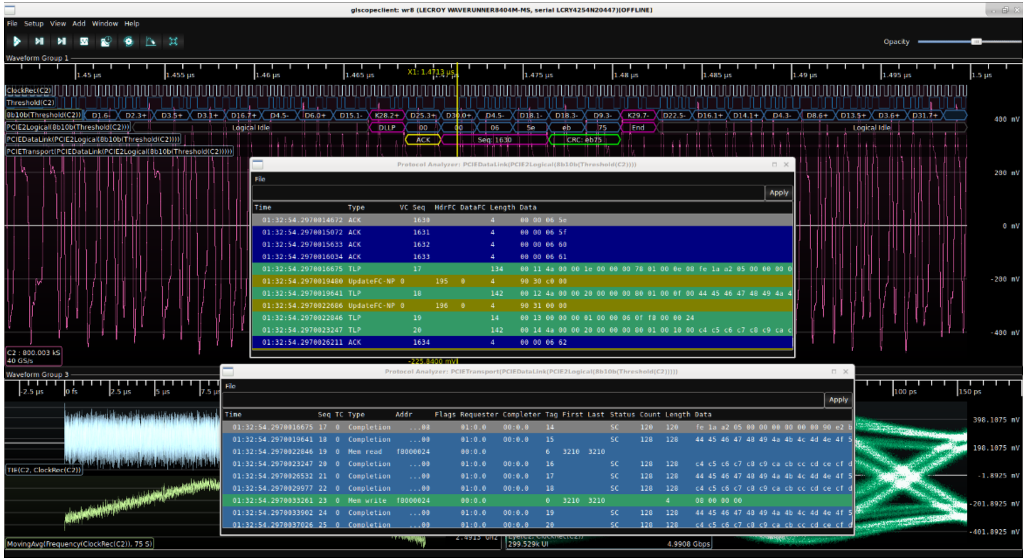
- MIPI DSI
- MIPI D-PHY



```
Time                     Width  Checksum   Image    Data
  09:20:19.9621539056 800    OK                   33 95 95 76 bb c2 ad
  09:20:19.9621865574 800    OK                   58 a3 a7 ac f2 fc 80
  09:20:19.9622192093 800    OK                   a0 e6 ef 99 de e7 38
  09:20:19.9622518612 800    OK                   a8 ed f7 4a 9c 9f 33
  09:20:19.9622845131 800    OK                   67 b0 b6 32 95 95 32
  09:20:19.9623171650 800    OK                   31 93 93 31 94 94 32
  09:20:19.9623498170 800    OK                   31 93 93 31 93 93 31
  09:20:19.9623824688 800    OK                   30 92 92 30 93 93 30
  09:20:19.9624151208 800    OK                   2f 92 92 2f 92 92 2f
  09:20:19.9624477727 800    OK                   2d 8e 91 2e 8e 91 2e
  09:20:19.9624804246 800    OK                   2d 8f 90 2d 90 90 2e
  09:20:19.9625130764 800    OK                   2d 8f 8f 2d 8f 8f 2d
  09:20:19.9625457284 800    OK                   2c 8e 8e 2c 8f 8f 2c
  09:20:19.9625783803 800    OK                   2b 8e 8e 2c 8e 8e 2c
  09:20:19.9626110322 800    OK                   2a 8d 8d 2b 8d 8d 2b
  09:20:19.9626436840 800    OK                   29 8b 8b 29 8c 8c 2a
  09:20:19.9626763359 800    OK                   28 8a 8a 28 8a 8a 29
  09:20:19.9627089878 800    OK                   27 89 89 27 8a 8a 28
  09:20:19.9627416398 800    OK                   26 88 88 27 89 89 27
  09:20:19.9627742917 800    OK                   26 88 88 26 88 88 26
  09:20:19.9628069436 800    OK                   25 87 87 25 87 87 26
  09:20:19.9628395955 800    OK                   23 85 85 24 86 86 24
  09:20:19.9628722474 800    OK                   22 84 84 23 85 85 23
  09:20:19.9629048993 800    OK                   21 83 83 22 83 83 22
  09:20:19.9629375512 800    OK                   21 82 82 21 83 83 45
  09:20:19.9629702031 800    OK                   20 81 81 24 85 85 8e
  09:20:19.9630028550 800    OK                   1e 7f 7f 6b c1 c1 a5
  09:20:19.9630355069 800    OK                   3e 8c 8c 9f fa fa a5
  09:20:19.9630681589 800    OK                   88 df df a3 ff ff a1
  09:20:19.9631008108 800    OK                   a1 fe ff a3 ff ff a5
  09:20:19.9631334625 800    OK                   a3 ff ff a4 ff ff a6
  09:20:19.9631661144 800    OK                   a1 ff ff a3 ff ff a4
  09:20:19.9631987664 800    OK                   a0 fe ff a0 ff ff a1
  09:20:19.9632314184 800    OK                   9f fe ff 9f fe ff a0
  09:20:19.9632640704 800    OK                   a1 ff ff a0 ff ff 9f
  09:20:19.9632967221 800    OK                   a3 ff ff a2 ff ff a1
```

PC

- DVI
- Intel eSPI
- PCIe gen 1 / 2
  - Gen 3+ planned
- USB low / full / high
  - SS planned

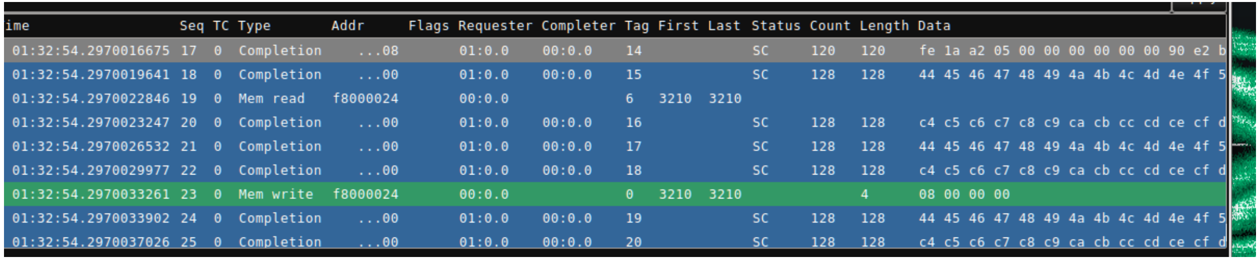


glscopeclient: wr8 (LECROY WAVERUNNER8404M-MS, serial LCRY4254N20447)[OFFLINE]
File Setup View Add Window Help
Opacity
Waveform Group 1
X1: 1.4713 µs
1.45 µs
1.455 µs
1.46 µs
1.465 µs
1.475 µs
1.48 µs
1.485 µs
1.49 µs
1.495 µs
1.5 µs
ClockRec(C2)
Threshold(C2)
8b10b(Threshold(C2))
D1.6- D2.3+ D3.5+ D3.1+ D16.7+ D4.5- D6.0+ D15.1- K28.2+ D25.3+ D30.0+ D4.5- D18.1- D18.3- D9.3- K29.7- D22.5- D16.1+ D14.1+ D4.3- D8.6+ D13.5+ D3.6+ D31.7+
PCIE2Logical(8b10b(Threshold(C2)))
Logical Idle
DLLP 00 00 06 5e eb 75 End
Logical Idle
PCIEDataLink(PCIE2Logical(8b10b(Threshold(C2))))
ACK
Seq: 1630
CRC: eb75
PCIETransport(PCIEDataLink(PCIE2Logical(8b10b(Threshold(C2)))))
400 mV
200 mV
0 mV
-200 mV
-400 mV
-225.8400 mV
C2 : 800.003 kS
40 GS/s
Waveform Group 3
-2.5 µs
0 fs
2.5 µs
5 µs
7.5 µs
TIE(C2, ClockRec(C2))
MovingAvg(Frequency(ClockRec(C2)), 75 S)
100 ps
150 ps
398.1075 mV
198.1075 mV
-1.8925 mV
-201.8925 mV
-401.8925 mV
299.529k UI
4.9908 Gbps

Protocol Analyzer: PCIEDataLink(PCIE2Logical(8b10b(Threshold(C2))))

```
Time                    Type         VC Seq   HdrFC DataFC Length Data
 01:32:54.2970014672 ACK              1630                4      00 00 06 5e
 01:32:54.2970015072 ACK              1631                4      00 00 06 5f
 01:32:54.2970015633 ACK              1632                4      00 00 06 60
 01:32:54.2970016034 ACK              1633                4      00 00 06 61
 01:32:54.2970016675 TLP              17                  134    00 11 4a 00 00 1e 00 00 00 78 01 00 0e 08 fe 1a a2 05 00 00 00 0
 01:32:54.2970019480 UpdateFC-NP 0          195   0       4      90 30 c0 00
 01:32:54.2970019641 TLP              18                  142    00 12 4a 00 00 20 00 00 00 80 01 00 0f 00 44 45 46 47 48 49 4a 4
 01:32:54.2970022686 UpdateFC-NP 0          196   0       4      90 31 00 00
 01:32:54.2970022846 TLP              19                  14     00 13 00 00 00 01 00 00 06 0f f8 00 00 24
 01:32:54.2970023247 TLP              20                  142    00 14 4a 00 00 20 00 00 00 80 01 00 10 00 c4 c5 c6 c7 c8 c9 ca c
 01:32:54.2970026211 ACK              1634                4      00 00 06 62
```

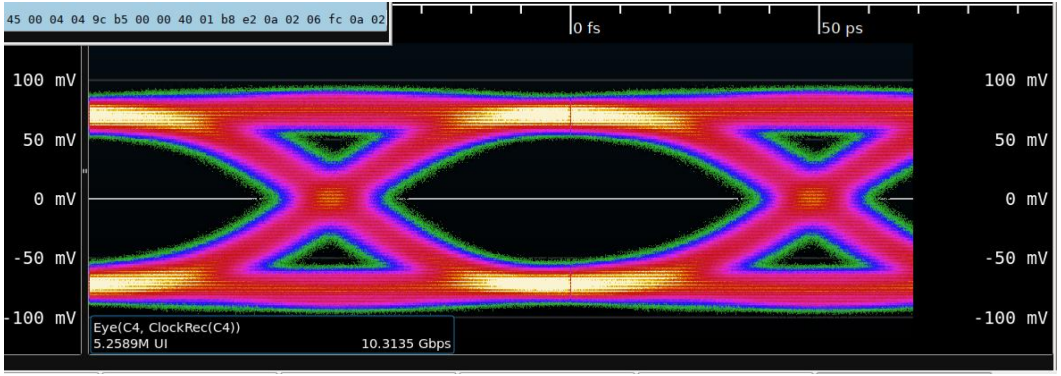
Protocol Analyzer: PCIETransport(PCIEDataLink(PCIE2Logical(8b10b(Threshold(C2)))))



```
ime                      Seq TC Type        Addr      Flags Requester Completer Tag First Last Status Count Length Data
 01:32:54.2970016675 17  0  Completion    ...08          01:0.0    00:0.0    14              SC     120   120    fe 1a a2 05 00 00 00 00 00 00 90 e2 b
 01:32:54.2970019641 18  0  Completion    ...00          01:0.0    00:0.0    15              SC     128   128    44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 5
 01:32:54.2970022846 19  0  Mem read     f8000024        00:0.0              6   3210  3210
 01:32:54.2970023247 20  0  Completion    ...00          01:0.0    00:0.0    16              SC     128   128    c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d
 01:32:54.2970026532 21  0  Completion    ...00          01:0.0    00:0.0    17              SC     128   128    44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 5
 01:32:54.2970029977 22  0  Completion    ...00          01:0.0    00:0.0    18              SC     128   128    c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d
 01:32:54.2970033261 23  0  Mem write    f8000024        00:0.0              0   3210  3210                4      08 00 00 00
 01:32:54.2970033902 24  0  Completion    ...00          01:0.0    00:0.0    19              SC     128   128    44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 5
 01:32:54.2970037026 25  0  Completion    ...00          01:0.0    00:0.0    20              SC     128   128    c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d
```

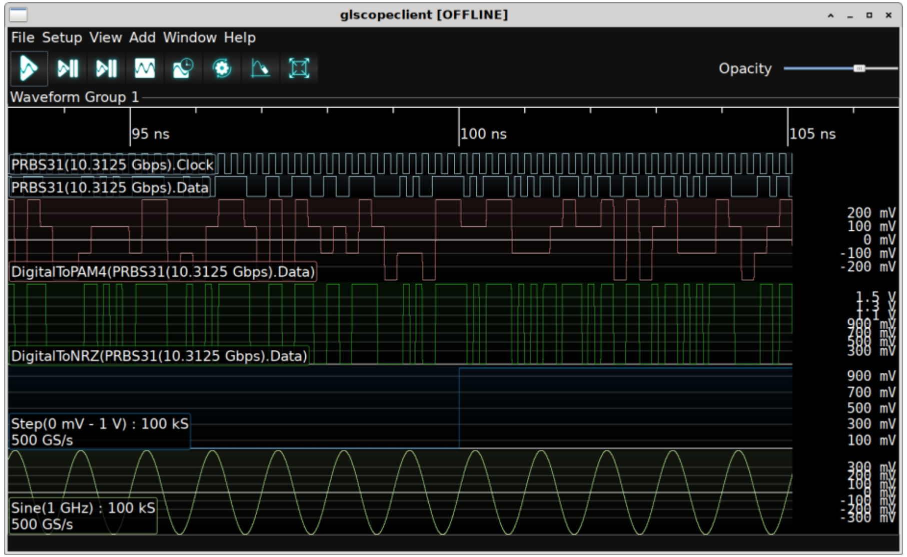
Signal integrity

- CTLE
- Channel emulation
- De-embed
- Emphasis insertion/removal
- Eye pattern
- Bathtub curves
- Jitter decomposition



Signal generation

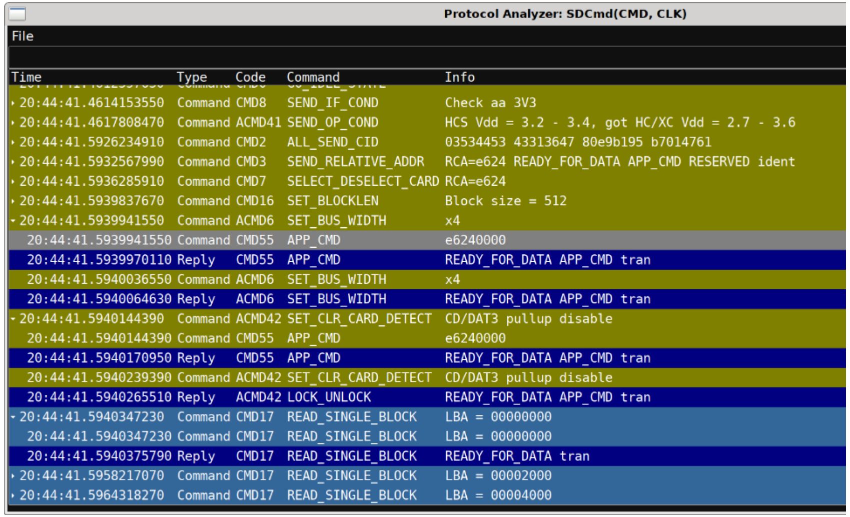
- Digital PRBS-7 / 15 / 23 / 31
- Digital to NRZ / PAM4
- AWGN
- Sine
- Step



Other features

Protocol analyzer

- Tabular display of packets
- Bidirectional sync
  - Click row to jump to packet
  - Drag timeline cursor
- Filtering



```
Time                 Type    Code   Command             Info
▸ 20:44:41.4614153550  Command CMD8   SEND_IF_COND        Check aa 3V3
▸ 20:44:41.4617808470  Command ACMD41 SEND_OP_COND        HCS Vdd = 3.2 - 3.4, got HC/XC Vdd = 2.7 - 3.6
▸ 20:44:41.5926234910  Command CMD2   ALL_SEND_CID        03534453 43313647 80e9b195 b7014761
▸ 20:44:41.5932567990  Command CMD3   SEND_RELATIVE_ADDR  RCA=e624 READY_FOR_DATA APP_CMD RESERVED ident
▸ 20:44:41.5936285910  Command CMD7   SELECT_DESELECT_CARD RCA=e624
▸ 20:44:41.5939837670  Command CMD16  SET_BLOCKLEN        Block size = 512
▾ 20:44:41.5939941550  Command ACMD6  SET_BUS_WIDTH       x4
   20:44:41.5939941550 Command CMD55  APP_CMD             e6240000
   20:44:41.5939970110 Reply   CMD55  APP_CMD             READY_FOR_DATA APP_CMD tran
   20:44:41.5940036550 Command ACMD6  SET_BUS_WIDTH       x4
   20:44:41.5940064630 Reply   ACMD6  SET_BUS_WIDTH       READY_FOR_DATA APP_CMD tran
▾ 20:44:41.5940144390  Command ACMD42 SET_CLR_CARD_DETECT CD/DAT3 pullup disable
   20:44:41.5940144390 Command CMD55  APP_CMD             e6240000
   20:44:41.5940170950 Reply   CMD55  APP_CMD             READY_FOR_DATA APP_CMD tran
   20:44:41.5940239390 Command ACMD42 SET_CLR_CARD_DETECT CD/DAT3 pullup disable
   20:44:41.5940265510 Reply   ACMD42 LOCK_UNLOCK         READY_FOR_DATA APP_CMD tran
▾ 20:44:41.5940347230  Command CMD17  READ_SINGLE_BLOCK   LBA = 00000000
   20:44:41.5940347230 Command CMD17  READ_SINGLE_BLOCK   LBA = 00000000
   20:44:41.5940375790 Reply   CMD17  READ_SINGLE_BLOCK   READY_FOR_DATA tran
▸ 20:44:41.5958217070  Command CMD17  READ_SINGLE_BLOCK   LBA = 00002000
▸ 20:44:41.5964318270  Command CMD17  READ_SINGLE_BLOCK   LBA = 00004000
```

Multi scope sync

- Cascade multiple instruments on common timebase
- Simple hardware setup
  - Common reference clock
  - Trigger in / out cascade
  - Touch probes to common point to calibrate delay
- Scopes don't have to be the same!

Getting Involved

Where to go?

- https://github.com/azonenberg/scopehal-apps
- IRC: #scopehal on libera.chat
- Discord: #scopehal on 1bitsquared

Acknowledgements

Industry Supporters

- Work for a scope vendor?
  - We welcome dev scopes, code contributions, and more!
- We've received contributions from:

pico® Technology

DIGILENT®

SIGLENT®

Contributors

- 9names
- Alyssa ‘noopwafel’ Milburn
- Anatol Ulrich
- Andres Manelli
- Antikerneldev
- Benjamin Vernoux
- Cody Holliday
- Dave Marples
- Dominik Sliwa
- Galen Schretlen
- Francisco Sedano
- Katharina B
- Kenley Cheung
- Mike Walters
- Nash Reilly
- Pepijn De Vos
- Robin Heinemann
- Rqou
- Sam210723
- Simon Richter
- Stephanie Wilde-Hobbs
- Sylvain Munaut
- Tarunik
- Tom Verbeure
- Unai Martinez-Corral
- Willem Melching
- Whitequark
- X44203
- xzcvczx

Questions?